Silicon Flatirons

KNOW WHAT'S NEXT.

Flatirons Report

Spectrum: Next Generation Interference Resolution and Enforcement

Jeffrey Westling and Alex Vetras

December 2016

Silicon Flatirons is a center for innovation at the University of Colorado Boulder to serve students, entrepreneurs, policymakers, and professionals at the intersection of law, policy, and technology.

This conference was held on September 15, 2016, in Boulder, Colorado.

Flatirons Reports capture thoughtful analysis of various issues in law, technology, and entrepreneurship. These reports are derived from research conducted by Silicon Flatirons faculty, fellows, and research assistants, as well as from thoughtful conference and roundtable conversations hosted by Silicon Flatirons that include academia, policymakers, legal professionals, entrepreneurs, and students sharing their knowledge and best practices on specific topics.

Flatirons Reports are published at siliconflatirons.org.

Executive Summary

With the rapid proliferation of wireless devices, enforcement of spectrum rights has come to the forefront of communications policy in recent years. Existing tools, however, may not be adequate to handle this influx of new technologies. New, inexpensive technologies that utilize spectrum present unique challenges for the FCC and operators using wireless spectrum.

To examine these issues, the Silicon Flatirons Center for Law, Technology and Entrepreneurship held a conference entitled *Spectrum: Next Generation Interference Resolution and Enforcement* with experts in the field on September 15, 2016. The participants generally agreed on the need for improvements in the interference dispute resolution process as devices become tightly packed in ever-narrowing bands. Furthermore, as participants discussed, the total number of emitters may be increasing the noise floor, degrading the performance of some devices using the wireless spectrum.

Participants explored ways that enforcement procedures can be improved to limit potential interference. They suggested a series of steps that could be implemented to achieve this goal. These include:

- Decentralizing enforcement to encourage private dispute resolution;
- Exploring the use of automation technology to prevent interference;
- Establishing identification tools for digital devices (e.g. a marker similar to a radio call sign); and
- Transitioning the Commission from an "analog agency" to one that focuses on enforcement in a digital age.

These steps, along with other suggestions detailed in the report, should aid in the process of identifying and preventing interference from occurring.

Table of Contents

Introduction

The Federal Communications Commission has the responsibility of managing and protecting non-federal radio operation. Professor Dale Hatfield, Senior Fellow at the Silicon Flatirons Center, set the stage for the Center's September 15, 2016 conference, *Spectrum: Next Generation Interference Resolution and Enforcement*, by introducing the basics of regulating radio spectrum, and positing both hypotheses and concerns regarding a radio-intensive future. The Commission, Hatfield explained, manages radio in four steps: allocation, definition of service rules, assignment, and enforcement.[1]

This conference focused on the fourth step: interference resolution and enforcement of the Commission's rules. Hatfield expressed concern that this step may currently be underappreciated by policy makers, an oversight that could lead to dire consequences given several emerging trends detailed below. In particular, he hypothesized that an explosive growth of devices and systems in closer proximity in frequency, space, and time will lead to an increased risk of harmful interference in the United States. Further, technological developments such as software defined radios present challenges to identifying and prosecuting attacks on critical infrastructure. Failure to enforce spectrum rules, therefore, endangers services critical to economic and social well-being.

Hatfield elaborated that because wireless networks are inherently open, they are subject to jamming and spoofing attacks.[2] As a result, the confidence in wireless technology may be decreasing. In a subsequent panel, Dr. Preston Marshall, Principal Wireless Architect for Google Access, observed that interference risks are driving a move away from putting life-critical functions on wireless networks.

Hatfield's and Marshall's remarks highlight several underlying questions of the conference: in light of increasing usage of and dependence on radio spectrum, how does the spectrum community measure, identify, and resolve harmful interference issues (both malicious and accidental)? And what, if anything, can be done ex ante to prevent harmful interference?

Answering these difficult questions is even more challenging when one considers, as conference participants contended, that the phrase "harmful interference" still lacks a clear definition beyond, "I know it when I see it." Additionally, participants and audience members stressed that more data is needed for measurement and improvement. Bryan Tramont, Managing Partner at Wilkinson Barker Knauer and Senior Fellow with Silicon Flatirons, emphasized the scarcity of data to draw from when he asked the conference attendees if a harmful interference case had ever been litigated. The answer, in short, was no. In raising this point, Tramont's goal was to spark discussion on how else we can gather the data we need, and with that data, better resolve spectrum interference issues. Drawing on their expertise and diverse experience, the

---

[1] JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS 89-96 (2nd ed. 2013); *see* Ellen P. Goodman, *Spectrum Rights in the Telecosm to Come*, 41 San Diego L. Rev. 269 (2004).

[2] Hatfield defines brute-force jamming as sending a powerful, interfering signal that obscures the desired signal. Spoofing, on the other hand, involves sending a fake signal, and is therefore much more difficult to perceive. For example, spoofing a GPS signal could lead navigation devices to believe a person or vehicle is in one location when they are really in another.

participants examined the state of spectrum enforcement today, and what opportunities exist for improvement in the future.

This report follows the thematic organization of the conference and collates participant and audience comments under the themes we believe to be most relevant. Section I takes stock of progress and challenges in spectrum enforcement, Section II discusses the use of technology to improve enforcement of spectrum usage, Section III analyzes the role of market and regulatory institutions in establishing a spectrum enforcement strategy, and Section IV concludes the report.

I. Taking Stock of the Progress and Challenges in Spectrum Enforcement

To understand what steps to take in improving enforcement, the first panel identified and explored the existing tools available to operators and enforcement personnel.[3] After identifying these tools, the discussion moved to existing and future challenges that will put a strain on the existing enforcement process.

A. Current Tools for Identifying and Resolving Interference

The participants first discussed the current tools that are available to identify and resolve interference. Such tools included private agreements, the use of harm claim thresholds, and the role of enforcement agents.

A primary method for ensuring that devices can operate without interference, which was first raised by Charla Rath, Vice President of Wireless Policy Development at Verizon, is private collaborative agreements. Private operators can negotiate with their neighbors (in terms of where the operator broadcasts, the frequency bands used, and the time in operation) to establish ex ante agreements about when, where, and how to operate to not cause harmful interference. Furthermore, private collaborative agreements can also be used ex post (i.e. after interference has occurred) to resolve an ongoing interference dispute. Underlying this argument is the notion that private operators can resolve their own interference disputes more easily, and at a lower cost, than seeking Commission intervention.

Participants also noted that when private operators negotiate amongst themselves, parties may incorporate the idea of harm claim thresholds to better describe the interference. A harm claim threshold is the theoretical in-band and out-of-band interfering signal levels that must be exceeded before a radio system can claim that it is experiencing harmful interference.[4] These thresholds can provide added clarity about the rights and responsibilities of radio service operators regarding harmful interference.[5] Though participants noted that harm claim thresholds remain relatively unused in front of the Commission, private parties use this idea of harm claim thresholds more often when negotiating with one another. As a result, these private

---

[3] Enforcement is a catch-all term that includes monitoring, complaint, adjudication, and remediation; see e.g. Jeffrey Westling, *Inter-party Interference Adjudication: Reactions from the Spectrum Community*, Spectrum: Next Generation Interference Resolution and Enforcement Conference (2016), http://siliconflatirons.org/publications/inter-party-interference-adjudication-reactions-from-the-spectrum-community/.

[4] FCC Technological Advisory Council, Interference Limits Policy and Harm Claim Thresholds: An Introduction (Mar. 5, 2014), http://transition.fcc.gov/oet/tac/tacdocs/reports/TACInterferenceLimitsIntrov1.0.pdf.

[5] Id. at 3.

operating agreements can better capture actual harm to a system and establish clear rules about when one party is violating such an agreement.

That is not to say that private collaborative agreements work perfectly or are the right solution in every situation.

- First, negotiated private collaborative agreements may not work when the two parties have different levels of bargaining power. For example, participants noted that new entrants may find it difficult to bring incumbents to the negotiating table as the incumbents have existing rights that they do not want to bargain away.

- Second, as discussed below, private negotiated agreements prevent data about interference events from being made publicly available.

- Finally, these negotiated agreements do little for unlicensed operators and devices because individual operators do not have the negotiating power, nor the legal justification, to prevent interference.

The participants noted that private collaborative agreements can only take the operator so far, and there will still need to be a "cop on the beat" who can identify and resolve instances where parties operate outside the rules and cause interference with their neighbors. Currently, the Commission's Enforcement Bureau is undergoing a modernization process, cutting back on the total number of field offices and personnel.[6] Limited resources prevent the Enforcement Bureau from addressing every interference dispute, but the field offices can still use existing tools to try and identify and resolve interference events. Charles Cooper, Acting Field Director at the Commission's Enforcement Bureau, noted that these tools include direction-finding vehicles and real-time spectrum analyzers.

As participants noted, the tools used will depend largely on the interference scenario being investigated. For example, continuous transmissions are generally easier for the investigator to identify than intermittent ones. Furthermore, even with the ideal tools, interference hunting is still largely an art given the complexity of the radio environment.

B. Existing and Upcoming Challenges Facing Spectrum Enforcement

Even with these tools, there are still many challenges that need to be addressed going forward. First, there is significant debate about the nature of the noise floor. Devices need to be able to separate the desired signal from the noise, and so the more noise in a system, the more difficult it is to operate successfully.[7] Some argue that the noise floor will increase with the increased proliferation of wireless devices, making device operation more difficult.[8]

---

[6] *See* Enforcement Bureau Enhances Procedures for Public Safety and Industry Interference Complaints, Public Notice, 30 FCC Rcd. 8574, 8575 (Aug. 17, 2015).

[7] *See generally* Office of Engineering and Technology Announces Technological Advisory Council (TAC) Noise Floor Technical Inquiry, Public Notice, 31 FCC Rcd. 6936 (June 15, 2016) ("Noise Floor Inquiry").

[8] Mark A McHenry et al., Electronic Noise Is Drowning Out the Internet of Things, IEEE (Aug. 18, 2015), http://spectrum.ieee.org/telecom/wireless/electronic-noise-is-drowning-out-the-internet-of-things.

First, as participants noted, this hypothetical increase in the noise floor has not been proven. The FCC Technological Advisory Council (TAC) recently launched an inquiry into this question.[9] As Anna Gomez, Partner at Wiley Rein LLP, suggested, until we gather more data, it will be hard to determine what will come out of the TAC research; Bryan Tramont added that getting any research funded has been a challenge.[10] To address this issue, Charla Rath suggested the Commission should open a proceeding with the goal of identifying best engineering practices, with the ultimate goal of reducing excess noise. This could give regulatory guidance on how manufacturers should design equipment.

Second, participants noted that aggregate interference from individual low-noise devices that together increase the noise floor present the challenge of identifying a wrongdoer. This challenge becomes more pronounced as the number of devices increase, especially unlicensed devices. Dale Hatfield gave the example of LED lights on a ballpark screen, where individual emitters do little harm but in the aggregate can cause harmful interference.

Finally, participants discussed the challenge of identifying offending devices due to the lack of public information about interference events or a database of devices that might be causing the interference an operator is experiencing. As Charles Cooper noted, "[y]ou have mixed services, and trying to differentiate which one may be causing interference and which is not is certainly a challenge and kind of brings to mind . . . the use of call signs . . . being able to identify these unlicensed devices." To better understand interference events and improve enforcement, regulators and researchers need case studies of current disputes. However, such case studies can be very difficult to come by.

Charla Rath expanded on the reason why commercial operators are unlikely to release interference data for public review. While companies want to protect their private information, a more significant concern for Rath was simply the administrative costs associated with reporting every interference event. Anna Gomez noted that companies also may be discouraged from publicly reporting an interference dispute to the Commission, because they do not want to reveal such information to competitors.

Rebecca Dorch, Senior Spectrum Policy Analyst in the Office of the Director at the National Telecommunications and Information Administration Institute for Telecommunications Sciences, also addressed the potential competitive effects on the device manufacturers themselves. If a single malfunctioning device is identified publicly, despite other instances of the same model not posing problems, then consumers may choose to avoid the product entirely. This would essentially punish the manufacturer for a single device's error. Furthermore, even if a database was created, Fred Wentland, Senior Vice President of Freedom Technologies, Inc., noted that it might not have access to licenses that are too old or not correctly located, or that the database just might not be in-depth enough to cover every device.

---

[9] Specifically, TAC is requesting responses to the following questions. 1). Is there a noise problem? 2). Where does the problem exist? 3). Is there quantitative evidence of the overall increase in the total integrated noise floor across various segments of the radio frequency spectrum? 4). How should a noise study be performed? Noise Floor Inquiry at 6937-6938.

[10] *See id.*

Despite these concerns, the total number of interference disputes and the issues that can arise remain relatively unclear. To improve enforcement capabilities, we believe better information about interference will be key.

An important question raised in the discussion was whether these enforcement tools will be adequate to handle the new challenges. Bryan Tramont suggested that the current enforcement tools are not adequate for these challenges, and Rebecca Dorch built on this by noting that many operators are moving to devices that transmit intermittently. As noted above, intermittent power devices are generally much more difficult for investigators to identify than traditional continuous power devices, and uncertainty remains with regard to how effective the enforcement agents can be.

II. Using Technology to Improve Enforcement

After analyzing the existing tools, the discussion moved to ways that technology could improve enforcement. John Chapin, Visiting Professor at Carnegie Mellon University's Department of Engineering and Public Policy, succinctly stated that the goal of using technology is to improve enforcement: to make enforcement cheaper, more effective, and faster, while still preserving key freedoms.[11] Today, we depend on an ever-increasing number of wireless devices and systems, yet are unable to afford an adequate amount of enforcement. Thus, we must find a way to lower the cost of enforcement to keep pace with the pervasiveness of these devices and systems. Chapin laid out his approach and the corresponding challenges for the panel to address in the form of the OODA loop decision cycle—Observe, Orient, Decide, and Act.

Observe. Chapin explained that in order to improve enforcement, we must first observe and measure interference issues. However, observation may become a difficult task to accomplish from a distance as systems become denser with short, low power links. Directional radiation of energy further complicates our ability to observe, because a sensor may not hear a nearby transmitter if its antenna is pointing in a different direction. To capture the data from all surrounding transmitters would require a costly and ubiquitous network of sensors.

Orient. In the orientation step, the measurements and data collected from observation are analyzed to make informed decisions. Pinpointing the origin of a transmission to a device or network is no simple undertaking. For example, many modern radios can rapidly change their operating frequency across multiple bands. In this increasingly common case, no static database will capture the owner of a transmission. Chapin noted that even if identification of the transmitter is possible, its owner may not be legally responsible for the transmission. He emphasized the ambiguity of ownership by asking the crowd who would be willing to take responsibility for every transmission emitted from every device they owned. It is not difficult to imagine cases, even beyond aggregate interference, where determining who is at fault may very well be impossible.

Decide and Act. The last two pieces of the OODA loop, decide and act, determine what to do with the data. This gets back to the underlying question: what does enforcement look like? Ultimately, the purpose of the loop is to come to enforcement conclusions, such as if any right or

[11] Remarks of John Chapin, The Biggest Challenges Facing Enforcement, Next Generation Interference Resolution and Enforcement (Sept. 15, 2016), http://www.silicon-flatirons.org/documents/conferences/2016-09-15%20Spectrum/ChapincommentstoSiliconFlatironsEnforcementWorkshop.pdf.

rules were violated and which party is responsible for resolving the issue. The action step may include intervention by an Enforcement Bureau representative, administrative and legal measures by the Commission, and potentially even the confiscation of interfering equipment by U.S. marshals.

Chapin concluded that this OODA loop, and its inherent challenges when it comes to resolving harmful interference, must be addressed within a framework of privacy and permission-less innovation. These key freedoms are potentially threatened by systems that collect a large amount of user data. Harry Surden, Associate Professor of Law at the University of Colorado, added that not only does law often impede or dampen future progress, but that policymakers usually make decisions without this consideration in mind. Essentially, Chapin and Surden urged the community to consciously balance its mission to improve enforcement with the preservation of anonymity for those staying within the service rules, and the continued encouragement of technological innovation.

Tom Power, Senior Vice President & General Counsel for CTIA, followed Chapin and Surden's remarks by pointing out that it may not be in the industry's best interest for the Commission to be forward-looking in its spectrum regulations. Even amidst surging demand for spectrum, Power suggested the Commission could potentially stifle innovation with anticipatory rules. Instead of predictive regulations, he recommended that the Commission continue to focus on promoting and accommodating disruptive technologies.

Within the framework of an ex post role for the Commission (that is, addressing new technologies and practices after they develop), participants offered several solutions to aid the Commission in combatting harmful interference in potentially more efficient ways. For example, embedded law, machine learning, digital identification, log-keeping, and time-limited leases were all suggested as at least partially automated options that the Commission could rely on to scale their spectrum enforcement.

Harry Surden explained that automated compliance—i.e., technology used to automate enforcement—can be divided into embedded law and machine learning. Surden described *embedded law* as computer-understandable laws. Embedded law involves translating law into logic understood by software and hardware and then embedding this computer code into applications and devices to ensure they stayed within the legal framework set forth by the federal government. Real-world examples of embedded law, Surden continued, include self-driving cars and even some software companies, for instance, TurboTax's IRS-acceptable translation of the personal income tax code.[12] Software-defined radios have also shown built-in compliance with spectrum-avoidance rules. These computer-code translations of law, if successful, would address

[12] Harry Surden, *Machine Learning and Law*, 89 Wash. L. Rev. 87, 88 (2014).

Chapin's challenge of making enforcement cheaper, effective, and faster by removing human discretion in many aspects of how to operate transmitters and receivers.

Marshall, while agreeing with the potential benefits of embedded law, raised the concern that even though the Commission may be adept at verifying that transmitters meet static

"The FCC has historically regulated a hardware-intensive industry, and in a very short period of time that has transitioned to become a software-intensive industry."
—John Chapin, Carnegie Mellon

specifications, checking behavior is a different challenge altogether. In working in the 3.5 GHz band for the Spectrum Access System, Marshall has faced the challenge of implementing potentially the most complex behavioral requirements ever promulgated by the Commission, both in the cloud and the device. He concluded that even the industry struggles to check behavior, which is demonstrated by the number of vulnerabilities found in software. Chapin observed that while the Commission has historically regulated a hardware-intensive industry, it is now confronted with a shift to a software-intensive industry. Thus, embedded law must overcome compliance obstacles not only in a specifications sense, but a behavioral sense as well.

Surden went on to explain that *machine learning* takes an artificial intelligence or statistical approach to enforcement. Through analyzing large amounts of data, machines can learn to detect rule violations. For example, this method is currently used by government agencies to help enforce financial law. In this context, machines have learned to notice when an individual takes a large position in a company just prior to a public announcement of its sale as potential insider trading. Similarly, machine learning could aid the Commission in detecting spectrum rule violations, identifying locations where illegal transmissions repeatedly occur. However, Surden noted that in a machine-learning environment, we need to be cognizant that sensitive data may be collected.

Cooper and Chapin also proposed implementing *station identification* (analog or digital), in which devices would broadcast a unique identifier. Chapin elaborated that to accomplish this and still ensure privacy, the ID would need to consist of an opaque bag of bits that changed in a non-predictable way over time. A database would then hold a corresponding key which, when combined with the bits and a timestamp, could be exchanged for the identity of the device. Chapin further added that we could couple identification with a black-box method that would have devices keep *logs* of their spectrum access decisions to facilitate efficient diagnosis of interference.

Beyond spotting interference, Chapin also recommended the use of time-limited leases to mitigate interference. In a *time-limited leases* methodology, devices could only transmit for a certain period of time, and then before transmitting again, the device would be forced to first

obtain a key.[13] Therefore, a mechanism would exist even for unlicensed devices to prevent continuous, unauthorized interference.

Each of these approaches, while not without their own challenges, presents creative ways to make enforcement cheaper, more effective, and faster, while still preserving key freedoms. Participants concluded that although there is no silver bullet, technology offers several promising avenues for improving the enforcement of spectrum technical and service rules.

III. The Role of Market and Regulatory Institutions

Finally, the participants looked at the role of market and regulatory institutions in improving spectrum enforcement. This included how to develop a regulatory approach to improve the enforcement of spectrum rights, exploring the role that interference avoidance can and should play in spectrum enforcement, and finally the differences between analog and digital enforcement.

A. Developing a Regulatory Approach

To address the challenges and issues described in Section I and the new tools and techniques in Section II, participants discussed how to develop a regulatory approach to improve enforcement of spectrum rights and to prevent interference to devices and operators. To that end, Preston Marshall of Google laid out four important considerations and strategies to make such improvements: (1) incentives for private monitoring; (2) creating a collaborative framework; (3) using and exploiting modern technology; and (4) establishing effective execution and penalization rules.

Private monitoring. Investigating and monitoring all spectrum use is too costly for the regulator to do alone. Commission resources are limited generally, and even more so after recent cutbacks to the enforcement bureau.[14] While, as participants noted, field offices do a good job of working with private operators to resolve interference disputes, a joint system of private monitors (such as the interference hunters who work to recognize RF signatures and trace them to a known interferer) and field office personnel may better monitor the airwaves while using less Commission resources.[15]

Bounties. To achieve such a system, Marshall suggested that regulators could potentially develop a bounty system to encourage private monitors. Under such a system, private operators who identify and report illegal transmissions would receive a reward. With the incentive to use their tools for monitoring, more eyes would be on the wireless spectrum, and the Commission would only need to expend resources when such transmissions were actually identified. To this point, Dr. Keith Gremban, Director of the NTIA's Institute for Telecommunications Services, suggested that a whole new industry could develop around a bounty system.

---

[13] John M. Chapin and William H. Lehr, *Time-Limited Leases for Innovative Radios*, Proceedings of 2007 2nd IEEE Int'l Symposium on New Frontiers in Dynamic Spectrum Access Networks, 606-19 (2007).

[14] Enforcement Bureau Enhances Procedures for Public Safety and Industry Interference Complaints, Public Notice, 30 FCC Rcd. 8574, 8575 (Aug. 17, 2015).

[15] Interference Hunting & Monitoring, ROHDE & SCHWARZ (last visited Oct. 25, 2016), http://www.rohde-schwarz-usa.com/IH.html.

Collaborative Framework. Building off this idea, Marshall suggested that a key aspect will be to create a *collaborative framework*. Under a collaborative framework, individuals can crowdsource to identify sources of interference. This idea can be exemplified by the Defense Advanced Research Projects Agency's Network Challenge, a contest in which ten weather balloons were placed in random locations across the country. DARPA offered a $40,000 cash prize to the first entrant who could submit the latitude and longitude of all ten balloons. To effectively locate and identify the ten balloons, participants worked together to collaboratively solve the problem. As Scientific American noted at the time,

> [t]he way people are networked socially via the Web today, they can be part of a team without necessarily leaving their homes or even living in the U.S. Some people might even do the legwork and then offer to give (or sell) information to participants, [Peter Lee, Transformational Convergence Technology Office Director] says.[16]

Participants noted that despite the estimation that this challenge would take around a month to complete, a team from MIT was able to crowdsource the data and correctly identify the ten balloons in mere hours.[17] Likewise, bounty programs used in the enforcement of spectrum rights could have a similar crowdsourcing component, further enhancing the speed at which sources of interference are identified. As Gremban noted, complexity will lead to an increased need for cooperation and while you can't identify every future dispute, every attribute you can identify will make the agreement better. Therefore, a collaborative framework will be vital to the effective enforcement of spectrum rights.

To achieve this collaborative system, people will need to use *technology* that can adequately identify these interfering signals. For example, software-defined radios present a significant challenge for regulatory agents due to their relatively low cost and increasing functionality. These new technologies that make private monitoring simpler and more affordable also raise the question of whether there is a correlation between automation and privatization. Rebecca Dorch noted that automation and privatization are both independent and related. As monitoring becomes more automated, private users will be able to utilize their technology for monitoring without actually having to engage in the monitoring themselves. Marshall further argued that with inexpensive software-defined radios, every device can be used in enforcement. For such a system to work, regulators will need to ensure that there is a source of *penalty* money available, which could be collected from prosecuting violators. This would allow bounty programs to be financially viable.

In addition, participants noted other steps and considerations that the regulator should take into account when developing a regulatory framework. For example, Paige Atkins, Associate Administrator, NTIA Office of Spectrum Management, suggested that such a framework could be modeled after the NIST Cybersecurity Framework, which consists of five concurrent and continuous functions—identify, protect, detect, respond and recover.[18] Participants also

---

[16] Larry Greenemeier, DARPA Challenge Competitors Already Mobilizing Social Network, SCIENTIFIC AMERICAN (Dec. 4, 2009), https://www.scientificamerican.com/article/darpa-network-challenge/.

[17] John C. Tang et al., *Reflecting on the DARPA Red Balloon Challenge*, 54 Communications of the ACM 78, 79 (2011), http://web.media.mit.edu/~cebrian/p78-tang.pdf.

[18] The NIST Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. *See also* Framework for Improving Critical Infrastructure Cybersecurity, National Institute

suggested that regulators should deploy and test these new technologies, particularly those used in spectrum sharing, to provide confidence that enforcement technologies will actually work.

Furthermore, participants argued that regulators should try and bring private operators onboard, though John Hunter, Senior Director of Technology and Engineering Policy at T-Mobile USA, suggested that it may be difficult to engage parties that are content with the current situation in developing new regulations. Finally, Paige Atkins suggested four areas that the community should consider: (1) building in enforcement; (2) encouraging good behavior; (3) devising a seamless and consistent regulatory framework; and (4) developing domestic solutions that can be extended internationally.

B. Interference Avoidance

The participants also discussed the role that interference avoidance can play in improving spectrum enforcement. Not all interference is harmful.[19] Therefore, license holders must expect and account for some level of noise, and react accordingly. By ensuring that the incumbent license holder can filter out these signals, interference issues will arise less often and therefore lower the

> *"Sharing mak[es] interference enforcement critical, [but] it also makes interference avoidance critical."*
> *—Paige Atkins, NTIA*

total amount of costs necessary to ensure compliance.

One solution, noted by some participants and rejected by others, would be to establish receiver standards that license holders must adhere to before complaining of harmful interference. David Redl, Chief Counsel, Communications and Technology, U.S. House Committee on Energy and Commerce, however, noted that this can be a difficult challenge, especially if devices are not managed after their sale. Essentially, because many companies that supply receivers do not control them after sale, there is little incentive for such companies to ensure that the receivers perform properly. Furthermore, receiver standards are just one way to increase receiver performance, and not necessarily a popular one. As Paige Atkins noted, it is not just enforcement, but also interference avoidance that can decrease spectrum interference.

C. Analog vs. Digital Enforcement

Another question raised throughout the discussion was how to ensure that the Commission can handle enforcement as the technology proceeds to a digital medium. John Chapin noted that the Commission is an analog agency in a digital age in terms of enforcement, meaning that the FCC has historically regulated a hardware intensive industry which has shifted

---

of Standards and Technology (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[19] FCC Technological Advisory Council, Basic Principles for Assessing Compatibility of New Spectrum Allocations 8-18 (Dec. 11, 2015), https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121015/Principles-White-Paper-Release-1.1.pdf.

to a software intensive industry. As a result, participants suggested that the Commission needs to transition into the digital age, using some of the technologies and strategies mentioned above.

For example, participants noted that privacy-centric regulators would be skeptical of implementing some of the suggestions such as automation and "digital license plates" because user data would be collected and stored. Paige Atkins noted, however, that sharing data will be key as we expand the capability of these technologies. Regulators will also need to address other issues such as the transition from static devices to devices that behave.

IV. Conclusion

A recurring note of the conference was that spectrum enforcement tools and techniques will need to evolve as radio use continues to increase. To better enforce the rights of radio operators, regulators should increase the amount of information available about previous interference events, use automation of technology to facilitate compliance with the rules, and develop a regulatory approach that incentivizes collaboration among private users to work in conjunction with the Commission's enforcement resources.

Appendix A: Spectrum Sharing

Participants discussed several topics during the conference that, while not directly related to spectrum enforcement, informed and supplemented the main issues that were covered in the report. This appendix supplements the report with those topics.

Clash of Cultures. David Redl raised what he described as the clash of cultures. On one side, companies such as Verizon or AT&T use spectrum as a primary part of their business, and therefore rely heavily on access to numerous frequency bands to serve their customers. On the other, edge providers, who provide applications to the end users using the underlying network, use spectrum access as an ancillary component to their business; while they aren't in the business of spectrum, these companies also rely on spectrum access. The challenge for regulators is balancing the economic interests of both sides and sharing the spectrum equitably.

In the context of LTE-U, for example, Wi-Fi proponents argue that there will be less bandwidth available for Wi-Fi no matter how well Wi-Fi and LTE-U co-exist. The primary business of wireless carriers pushing LTE-U technology is selling spectrum access, while Wi-Fi is being promoted by organizations primarily interested in ensuring that their customers have internet access (e.g. municipalities, cable operators and edge providers). As a result, Redl explained, their incentives are at odds and their expectations are in conflict.

Sharing Technology. Participants also discussed coexistence arrangements like federal/non-federal band sharing that could in turn reduce the enforcement burden. To facilitate and encourage sharing, participants noted that it is critical for the community to build trust that sharing technology will work. Without confidence that interference will be avoided and problems resolved, agreements between parties will not occur due to the uncertainty about spectrum rights. Paige Atkins noted that it would take time for stakeholders (especially protected incumbents) to develop confidence that new sharing technologies were reliable. The point was also made in the discussion that sharing arrangements that work in one band cannot simply be applied to another band.

Forced Sharing. Rich Kaplan explained that it is important to consider who can be good sharing partners before new sharing regimes are imposed. He noted that private sharing agreements generally work better than sharing mandated by the Commission. This ties back into the clash of cultures model: incentives to share may not always be sufficient to facilitate these private agreements.

Kaplan adduced past sharing case studies as examples. He argued that the TV white space sharing plan failed to produce the promised benefits, primarily due to the nature of the parties who were sharing the spectrum. Broadcasters were inherently skeptical of the unlicensed users operating in the white space between channels, and did not know who to call on in the event that they experienced interference. In contrast, the Department of Defense found a home in the Broadcast Auxiliary Services (BAS) band used for electronic news gathering by working with broadcasters. Due to the relatively intermittent and geographically separate use of the band by both broadcasters and the military, both parties can use the band effectively with few issues. Kaplan noted that this sharing was not mandated, and argued that in general sharing plans that are not mandated by the FCC operate more successfully than those that are.

Public Pressure. Finally, Redl described a relatively new phenomenon occurring in the field: these new technology issues are becoming mainstream. As a result, there is more of a push by the citizenry that applies political pressure on the regulator. As Redl noted, this has been a major factor in the LTE-U debate because many consumers do not want to see their Wi-Fi interrupted. The challenge we are facing now, as he described, is how to make the "economics square." Going forward, pressure from everyday consumers may play an increasing role in enforcement priorities and strategies.

Speakers

Introduction

Dale Hatfield
Spectrum Initiative Co-Director, Senior Fellow
Silicon Flatirons
Adjunct Professor
University of Colorado

Pierre de Vries (moderator)
Spectrum Initiative Co-Director, Senior Fellow
Silicon Flatirons

Panel 1: Taking stock - progress and challenges

Charles Cooper
Acting Field Director, Enforcement Bureau
Federal Communications Commission

Anna Gomez
Partner
Wiley Rein LLP

Charla Rath
Vice President - Wireless Policy Development
Verizon

Fred Wentland
Senior Vice President
Freedom Technologies, Inc.

Rebecca Dorch (moderator)
Senior Spectrum Policy Analyst
Office of the Director
NTIA Institute for Telecommunication Sciences

Panel 2: The use of technology to improve enforcement

John Chapin
Visiting Professor, Department of Engineering and Public Policy
Carnegie Mellon University
Senior Consultant
Roberson and Associates

Preston Marshall
Principal Wireless Architect
Google Access

Thomas Power
Senior Vice President & General Counsel
CTIA - The Wireless Association

Harry Surden
Associate Professor of Law
University of Colorado

Keith Gremban (moderator)
Director
NTIA Institute for Telecommunications Sciences

Panel 3: The role of market and regulatory institutions

Paige Atkins
Associate Administrator
NTIA Office of Spectrum Management

John Hunter
Senior Director of Technology and Engineering Policy
T-Mobile USA

Rick Kaplan
Executive Vice President, Strategic Planning
National Association of Broadcasters

David Redl
Chief Counsel, Communications and Technology
U.S. House Committee on Energy and Commerce

Bryan Tramont (moderator)
Managing Partner
Wilkinson Barker Knauer, LLP
Senior Fellow
Silicon Flatiron